

### **Amendments To The Claims**

This listing of claims will replace all prior versions, and listings, of claims in the application:

#### **Listing of Claims:**

Claims 1-3 (canceled)

Claim 4 (previously presented): An apparatus comprising:

- a first encryption key storage unit configured to store a first encryption key;
- a second encryption key storage unit configured to contain a second encryption key;
- an encryption unit configured to encrypt a message containing the first encryption key, the message encrypted with the second encryption key;
- a radio configured to transmit the message over a wireless network and configured to receive a subsequent message over the wireless network, the subsequent message encrypted with the first encryption key;
- a decryption unit configured to decrypt the subsequent message received from the radio; and
- a protocol management unit configured to convey the subsequent message to a host device, wherein the apparatus further comprises:
  - a selector configured to select between the encryption key storage units as input to the encryption unit and decryption unit.

Claim 5 (original): The apparatus of claim 4, further comprising:

- a device control unit configured to aid the selector in the selection between the encryption key storage units.

Claim 6 (original): The apparatus of claim 5 wherein the second encryption key is symmetric.

Claim 7 (original): The apparatus of claim 6 wherein the first encryption key is symmetric.

Claim 8 (currently amended): The apparatus of claim 4 [[1]] wherein the second encryption key is a peripheral device encryption key.

Claim 9 (original): The apparatus of claim 8 wherein the first encryption key is a host device encryption key.

Claim 10 (currently amended): The apparatus of claim 9 wherein the peripheral device encryption key is received by the [[a]] host device via input by a user.

Claim 11 (previously presented): The apparatus of claim 10, wherein the protocol management unit is configured to convey the subsequent message to the host device via the Universal Serial Bus protocol.

Claim 12 (currently amended): A method comprising:

receiving, at a module, a second encryption key;

storing the second encryption key in a second encryption key storage unit;

selecting the second encryption key from the second encryption key storage unit as an encryption input;

transmitting, from the module, a message containing a first encryption key over a wireless network, the message encrypted with the second encryption key; [[and]]

selecting the first encryption key from the first encryption key storage unit as a decryption input;

receiving, at the [[a]] module, a subsequent message encrypted with the first encryption key;

decrypting the subsequent message with the first encryption key; and

conveying the subsequent message to a host device.

Claim 13-14 (canceled)

Claim 15 (currently amended): The method of claim [[14]] 12 wherein the second encryption key is

symmetric.

Claim 16 (currently amended): The method of claim [[15]] 12 wherein the first encryption key is symmetric.

Claim 17 (previously presented): The method of claim 12 wherein the second encryption key is a peripheral device encryption key.

Claim 18 (original): The method of claim 17 wherein the first encryption key is a host device encryption key.

Claim 19 (currently amended): The method of claim 18 wherein the peripheral device encryption key is received by the [[a]] host device via input by a user.

Claim 20 (canceled)

Claim 21 (currently amended): The method of claim [[20]] 18 wherein the first encryption key storage unit that stores the host device encryption key is a read only memory.

Claim 22 (currently amended): The method of claim 21 further comprising:

sending the decoded subsequent message to the [[a]] host device using a Universal Serial Bus interface.

Claim 23 (currently amended): A computer-readable medium encoded with data and instructions, the data and instructions causing an apparatus executing the instructions to:

receive, at a module, a second encryption key;  
store the second encryption key in a second encryption key storage unit;  
select the second encryption key from the second encryption key storage unit as an encryption input;

transmit, from the module, a message containing a first encryption key over a wireless network, the message encrypted with the second encryption key; [[and]]

select the first encryption key from the first encryption key storage unit as a decryption input;

receive, at the module, a subsequent message encrypted with the first encryption key;

decrypt the subsequent message with the first encryption key; and

convey the subsequent message to a host device.

Claim 24 – 25 (canceled)

Claim 26 (currently amended): The computer-readable medium of claim 23 [[25]] wherein the second encryption key is symmetric.

Claim 27 (original): The computer-readable medium of claim 26 wherein the first encryption key is symmetric.

Claim 28 (previously presented): The computer-readable medium of claim 23 wherein the second encryption key is a peripheral device encryption key.

Claim 29 (original): The computer-readable medium of claim 28 wherein the first encryption key is a host device encryption key.

Claim 30 (currently amended): The computer-readable medium of claim 29 wherein the peripheral device encryption key is received by the [[a]] host device via input by a user.

Claim 31 (canceled)

Claim 32 (original): The computer-readable medium of claim 29 wherein the encryption key storage unit that stores the host device encryption key is a read only memory.

Claim 33 (currently amended): The computer-readable medium of claim 32, the instructions further causing an apparatus executing the instructions to:

    sending the decoded subsequent message to the [[a]] host device using a Universal Serial Bus interface.

Claim 34 (currently amended): An apparatus comprising:

    means for receiving, at a module, a second encryption key;

means for storing the second encryption key in a second encryption key storage unit;

means for selecting the second encryption key from the second encryption key storage unit as an encryption input;

    means for transmitting, from the module, a message containing a first encryption key over a wireless network, the message encrypted with the second encryption key; [[and]]

means for selecting the first encryption key from the first encryption key storage unit as a decryption input;

    means for receiving, at the module, a subsequent message encrypted with the first encryption key;

means for decrypting the subsequent message with the first encryption key; and

means for conveying the subsequent message to a host device.

Claim 35 – 36 (canceled)

Claim 37 (currently amended): The apparatus of claim 34 [[36]] wherein the second encryption key is symmetric.

Claim 38 (original): The apparatus of claim 37 wherein the first encryption key is symmetric.

Claim 39 (previously presented): The apparatus of claim 34 wherein the second encryption key is a peripheral device encryption key.

Claim 40 (previously presented): The apparatus of claim 39 wherein the first encryption key is a host device encryption key.

Claim 41 (currently amended): The apparatus of claim 40 wherein the peripheral device encryption key is received by the [[a]] host device via input by a user.

Claims 42-43 (canceled):

Claim 44 (original): The apparatus of claim 43 further comprising:  
means for decrypting received messages.

Claim 45 (original): The apparatus of claim 44 further comprising:  
means for encrypting messages to be transmitted.

Claim 46 (currently amended): The apparatus of claim 45 further comprising:  
means for sending the decoded subsequent message to the [[a]] host device using a Universal Serial Bus interface.

Claim 47 – 49 (canceled):

Claim 50 (previously presented): An apparatus comprising:  
a first encryption key storage unit configured to contain a first encryption key;  
a radio configured to receive a message over a wireless network from a host and to transmit a subsequent message over the wireless network, the received message encoded with the first encryption key and containing a second encryption key, the subsequent message encrypted with the second encryption key;  
a decryption unit configured to decrypt the received message with the first encryption key;  
at least one temporary key storage unit configured to store the second encryption key;  
an encryption unit configured to encrypt the subsequent message with the second encryption

key; and

wherein the radio is further configured to receive data messages over the wireless network from the host, the data message encoded with the second encryption key; and

wherein the apparatus further comprises:

a selector configured to select between the encryption key storage units as input to the encryption unit and decryption unit.

Claim 51 (original): The apparatus of claim 50, further comprising:

a device control unit configured to aid the selector in the selection between the encryption key storage units.

Claim 52 (original): The apparatus of claim 51, further comprising:

a protocol management unit configured to convey the data message to a peripheral device.

Claim 53 (original): The apparatus of claim 52, wherein the protocol management unit is configured to convey the data message to a peripheral device via the Universal Serial Bus protocol.

Claim 54 (original): The apparatus of claim 53 wherein the first encryption key is symmetric.

Claim 55 (original): The apparatus of claim 54 wherein the second encryption key is symmetric.

Claim 56 (currently amended): The apparatus of claim 50 [[47]] wherein the first encryption key is a peripheral device encryption key.

Claim 57 (original): The apparatus of claim 56 wherein the second encryption key is a host device encryption key.

Claim 58 (currently amended): A method comprising:

receiving a message over a wireless network from a host, the message encoded with a first

encryption key and containing a second encryption key;

decrypting the received message using the first encryption key selected as a decryption input from a first encryption key storage unit storing the first encryption key, extracting the second encryption key;

storing the second encryption key in a second encryption key storage unit;

selecting the second encryption key from the second encryption key storage unit as an encryption input;

encrypting subsequent messages with the second encryption key; and

sending the encrypted subsequent messages to the host over the wireless network.

Claim 59 - 60 (canceled)

Claim 61 (currently amended): The method of claim 58 ~~[[59]]~~ wherein the first encryption key is symmetric.

Claim 62 (original): The method of claim 61 wherein the second encryption key is symmetric.

Claim 63 (previously presented): The method of claim 58 wherein the first encryption key is a peripheral device encryption key.

Claim 64 (original): The method of claim 63 wherein the second encryption key is a host device encryption key.

Claim 65 (currently amended): The method of claim 64 wherein the second encryption key storage unit is a register.

Claim 66 (original): The method of claim 65 wherein the encrypted messages sent to the host are received through a Universal Serial Bus interface.



Claim 67 (currently amended): A computer-readable medium encoded with data and instructions, the data and instructions causing an apparatus executing the instructions to:

receive a message over a wireless network from a host, the message encoded with a first encryption key and containing a second encryption key;

decrypt the received message using the first encryption key selected as a decryption input from a first encryption key storage unit storing the first encryption key, extracting the second encryption key;

store the second encryption key in a second encryption key storage unit;

select the second encryption key from the second encryption key storage unit as an encryption input;

encrypt subsequent messages with the second encryption key; and

send the encrypted subsequent messages to the host over the wireless network.

Claim 68 - 69 (canceled)

Claim 70 (currently amended): The computer-readable medium of claim 67 ~~[[68]]~~ wherein the first encryption key is symmetric.

Claim 71 (original): The computer-readable medium of claim 70 wherein the second encryption key is symmetric.

Claim 72 (previously presented): The computer-readable medium of claim 67 wherein the first encryption key is a peripheral device encryption key.

Claim 73 (original): The computer-readable medium of claim 72 wherein the second encryption key is a host device encryption key.

Claim 74 (original): The computer-readable medium of claim 73 wherein the encryption key storage unit is a register.

Claim 75 (previously presented): The computer-readable medium of claim 73 wherein the encrypted messages sent to the host were received through a Universal Serial Bus interface.

Claim 76 (currently amended): An apparatus comprising:

means for receiving a message over a wireless network from a host, the message encoded with a first encryption key and containing a second encryption key;

means for decrypting the received message using the first encryption key selected as a decryption input from a first encryption key storage unit storing the first encryption key, extracting the second encryption key;

means for storing the second encryption key in a second encryption key storage unit;

means for selecting the second encryption key from the second encryption key storage unit as an encryption input;

means for encrypting subsequent messages with the second encryption key; and

means for sending the encrypted subsequent messages to the host over the wireless network.

Claim 77 (original): The apparatus of claim 76 further comprising:

means for storing the first encryption key.

Claim 78 - 79 (canceled)

Claim 80 (currently amended): The apparatus of claim 77 ~~[[78]]~~ wherein the first encryption key is symmetric.

Claim 81 (original): The apparatus of claim 80 wherein the second encryption key is symmetric.

Claim 82 (previously presented): The apparatus of claim 76 wherein the first encryption key is a peripheral device encryption key.

Claim 83 (original): The apparatus of claim 82 wherein the second encryption key is a host device encryption key.

Claim 84 (original): The apparatus of claim 83 wherein the means for storing the second encryption key is a register.

Claim 85 (original): The apparatus of claim 84 wherein the encrypted messages sent to the host were received through a Universal Serial Bus interface.

Claim 86 (currently amended): The apparatus of claim 4 [[1]] wherein the first encryption key is specific to the [[a]] host device coupled to the radio.

Claim 87 (currently amended): The method of claim 12 wherein the first encryption key is specific to the [[a]] host device coupled to the module.

Claim 88 (currently amended): The computer-readable medium of claim 23 wherein the first encryption key is specific to the [[a]] host device coupled to the module.

Claim 89 (currently amended): The apparatus of claim 34 wherein the first encryption key is specific to the [[a]] host device coupled to the module.

Claim 90 (currently amended): The apparatus of claim 50 [[47]] wherein the second encryption key is specific to the host.

Claim 91 (previously presented): The method of claim 58 wherein the second encryption key is specific to the host.

Claim 92 (previously presented): The computer-readable medium of claim 67 wherein the second encryption key is specific to the host.

Claim 93 (previously presented): The apparatus of claim 76 wherein the second encryption key is specific to the host.